Proving modern code-based dual attacks

Charles Meyer-Hilfiger*[1]

[1]Université de Rennes, Irisa – Univ Rennes, CNRS, Inria, IRISA - UMR 6074 – France

Résumé

In code-based cryptography, dual attacks have recently been improved. They are now competitive for solving the decoding problem and beat information-set decoders for a significant regime. These recent attacks, starting from Carrier et al. (Asiacrypt 2022), work by reducing decoding to an LPN problem where the secret and the noise involve parts of the error vector coming from the decoding problem. While in the original Asiacrypt 2022 work an LPN modeling was used to carry out the analysis, Meyer-Hilfiger and Tillich (TCC 2023) showed that this model could not be used. This TCC paper then proposed a new way to analyze this attack by using Fourier theory and by modeling the weight enumerator of a random linear code as a Poisson variable. The analysis of the newest and most efficient dual attack, doubleRLPN, introduced by Carrier et al. (Eurocrypt 2024), also relies on this technique and on this model (that was verified experimentally). All in all, the analysis of these attacks is heuristic at the moment.
Our main contribution is to devise a variant of doubleRLPN that we can fully prove without using any model. More, we show that our variant has the same performance, up to polynomial factors, as the original doubleRLPN algorithm. Our algorithm and its analysis are also simpler. Our technique involves flipping the coordinates of the noisy codeword and observing the fine changes in the amount of noise of the related LPN problem to reconstruct the entire error. The analysis is based on the second-order behavior of the bias of the noise, which was already used in the original analysis. This technique could be slightly generalized to analyze lattice-based dual attacks.

*Intervenant